دورة تركيب و صيانة أنظمة المراقبة

CCTV Systems

الوحدة الثالثة

1. مقدمة

بعد اكتمال التوصيلات الفيزيائية وتمديد الكابلات وتغذية الكاميرات بالطاقة، يأتي الدور على "الروح البرمجية" للنظام. إن عملية البرمجة وإعداد الشبكة هي التي تمنح نظام المراقبة قيمته الحقيقية؛ حيث تحول الأجهزة من مجرد شاشات عرض محلية مغلقة داخل غرفة التحكم، إلى منظومة ذكية يمكن إدارتها، واستقبال تنبيهاتها، واستعراض لقطاتها الحية من أي مكان في العالم عبر الهواتف الذكية والحواسب.

2. أولاً: الإعدادات الأساسية وتشغيل النظام لأول مرة (Initialization)

عند تشغيل جهاز التسجيل (DVR / XVR / NVR) لأول مرة، يمر الفني بمرحلة التهيئة الأساسية، وتتضمن الخطوات التالية:

١. **تعيين كلمة المرور (Password Creation):** لم تعد الأجهزة الحديثة تأتي بكلمات مرور افتراضية (مثل 12345 أو admin) لأسباب أمنية. يجب تعيين كلمة مرور معقدة تحتوي على حروف وأرقام ورموز لمنع اختراق النظام.
٢. **ضبط الوقت والتاريخ (Date Time):** خطوة بالغة الأهمية من الناحية القانونية والجنائية؛ فالتاريخ والوقت الخاطئ يجعل التسجيلات غير

مقبولة كدليل رسمي. يُفضل تفعيل بروتوكول الوقت الشبكي (NTP - Network Time Protocol) ليقوم الجهاز بتحديث وقته تلقائياً عبر الإنترنت.

٣ **تهيئة القرص الصلب (HDD\ Formatting):** يتم مسح الهارد ديسك الجديد وتقسيمه بواسطة نظام ملفات الجهاز ليصبح جاهزاً للكتابة المستمرة.

٤ **جدولة التسجيل (Recording\ Schedule):** تحديد آلية عمل الكاميرات:
   - **التسجيل المستمر (Continuous):** التسجيل على مدار 24 ساعة.
   - **استشعار الحركة (Motion Detection):** يبدأ الجهاز بالتسجيل فقط عند رصد حركة في الكادر، مما يوفر مساحة ضخمة من الهارد ديسك ويسهل عملية البحث عن الأحداث لاحقاً.

3. ثانياً: هندسة الشبكة المحلية (LAN Settings) لأنظمة الـ IP

في أنظمة المراقبة الشبكية (IP CCTV)، تصبح الكاميرات وجهاز التسجيل عبارة عن أجهزة كمبيوتر مصغرة داخل شبكة محلية. لضمان تواصلها دون مشاكل، يجب ضبط المعطيات التالية:

1. عناوين الـ IP واستراتيجية التوزيع

- **بروتوكول الـ DHCP:** يقوم الراوتر بتوزيع عناوين IP تلقائية للأجهزة.
  تنبيه: يُمنع تفعيل هذه الخاصية لأجهزة التسجيل أو كاميرات الـ IP، لأن تغيير الـ IP تلقائياً عند إعادة تشغيل الراوتر سيؤدي إلى فقدان الاتصال بالكاميرات (Video Loss).

- **العناوين الثابتة (Static IP):** يجب تثبيت عنوان IP يدوي لكل كاميرا ولجهاز التسجيل لضمان استقرار الاتصال.

2. تجنب تعارض العناوين (IP Conflict)

إذا أخذت كاميرتان نفس عنوان الـ IP (مثلاً 192.168.1.50)، ستتوقف الصورة وتظهر وتختفي بشكل متقطع. يتم حل هذه المشكلة باستخدام برامج فحص الشبكة الخاصة بالشركات المصنعة مثل:

- برنامج **SADP Tool** لشركة *Hikvision*.
- برنامج **ConfigTool** لشركة *Dahua*.

تتيح هذه الأدوات للفني رؤية جميع الكاميرات المعلقة في الشبكة وتعديل عناوينها الفرعية (Subnet) لتتوافق مع نطاق الراوتر وجهاز الـ NVR.

4. ثالثاً: الربط بالإنترنت والمراقبة عن بُعد (Remote Viewing)

توجد طريقتان رئيسيتان لربط نظام المراقبة بالإنترنت ليعمل على الهاتف المحمول:

الطريقة الأولى: التقنية السحابية (P2P / Cloud) - الأكثر شيوعاً

تعتمد على سيرفر وسيط توفره الشركة المصنعة للكاميرات.

- **آلية العمل:** يتم تفعيل خاصية الـ $P2P$ من إعدادات الشبكة في الجهاز، ليقوم بتوليد رمز استجابة سريعة ($QR\ Code$) فريد وخاص به.

طريقة التفعيل: يقوم المستخدم بتحميل تطبيق الهاتف المعتمد (مثل *Hik-Connect* أو *DMSS*)، ثم مسح الـ $QR\ Code$ بكاميرا الهاتف. يتصل الهاتف بالسيرفر السحابي الذي يربطه مباشرة بجهاز التسجيل في المنزل دون الحاجة لأي إعدادات معقدة في الراوتر.

- **المميزات:** مجانية بالكامل، تعمل على أي اشتراك إنترنت، وآمنة للغاية وسهلة التطبيق.

الطريقة الثانية: توجيه المنافذ (Port Forwarding) - للمشاريع الكبرى

- **المتطلبات:** تتطلب حجز عنوان إنترنت ثابت من شركة الاتصالات يُسمى Static Public IP.
- **آلية العمل:** يتم الدخول إلى لوحة تحكم راوتر الموقع، وعمل "توجيه" أو فتح للمنافذ (Ports) الخاصة بجهاز التسجيل (مثل بورت الـ *HTTP* وبورت الـ *RTSP* المسؤول عن بث الفيديو).
- **المميزات:** سرعة استجابة أعلى وبث أنعم للفيديو، والقدرة على ربط الكاميرات ببرامج إدارة الفيديو الاحترافية (VMS) عبر فروع متباعدة.

5. رابعاً: البروتوكولات والمعايير البرمجية العالمية

لضمان توافق الأجهزة من شركات مختلفة، تعتمد الأنظمة على بروتوكولات موحدة:

١. **معيار ONVIF (Open Network Video Interface Forum):** هو بروتوكول عالمي يسمح لكاميرا IP من شركة (مثل *Dahua*) بالعمل والتسجيل على جهاز NVR من شركة أخرى (مثل *Hikvision*) بكامل

من مصنع واحد.

٢ **بروتوكول RTSP (Real-Time Streaming Protocol):** البروتوكول المسؤول عن تشفير ودفق الفيديو الحي عبر الشبكة لتتمكن التطبيقات ومتصفحات الإنترنت من عرضه بسلاسة.

6. خامساً: الأمن السيبراني لأنظمة المراقبة (Cybersecurity)

بما أن نظام المراقبة متصل بالإنترنت، فإنه عرضة لمشكلات الاختراق والتجسس إذا لم يتم تأمينه برمجياً:

- **تغيير المنافذ الافتراضية:** يُنصح بتغيير بورتات الجهاز الشهيرة (مثل بورت 80 أو 8000) إلى أرقام عشوائية معقدة لمنع برامج الفحص الآلية من العثور على الجهاز.
- **تحديث الفيرموير (Firmware Update):** تحديث نظام تشغيل الـ DVR/NVR بشكل دوري لسد الثغرات الأمنية التي يكتشفها المخترقون.
- **تعطيل بروتوكول UPnP:** يفضل إغلاقه من الراوتر لأنه يقوم بفتح منافذ تلقائية قد تشكل ثغرة في جدار الحماية.

7. الخلاصة

إن برمجة نظام الـ CCTV وإعداده شبكياً لا تقل أهمية عن جودة الكاميرات نفسها. النجاح في هذا الجانب يضمن للموقع استقراراً في البث، وحماية قصوى للبيانات من الاختراق، والوصول الفوري والسهل للأحداث من أي مكان في العالم، مما يحقق الهدف الحقيقي من المنظومة الأمنية المتكاملة.

روابط كتيبات دليل المستخدم و دليل إرشادي لمنتجات شركة Hikvision و شركة *Dahua*

https://www.hikvision.com/ar/support/download/marketing-materials/

https://www.hikvision.com/content/dam/hikvision/ca/how-to-document/How-to-download-and-use-the-SADP-tool.pdf

https://support.dahuasecurity.com/en

https://www.dahuasecurity.com/ar/products

By:Haytham Zeidan

https://archive.org/details/@wazefapress